DCAA RULES FOR COMPUTER USERS

February 14, 2012
(Updated in accordance with DoD guidance dated May 9, 2008)

Introduction and Guidance
The following rules for computer users will be provided initially to all DCAA employees and contractors and subsequently to all new DCAA employees and contractors for their review, retention and signature. Much of the basis for these Rules for Computer Users is contained in DCAAR 4140.2 and DOD Instruction 8500.2.

References
OMB Circular A-130 Management of Federal Information Resources, November 28, 2000 (note: DCAA Rules for
Computer Users implements OMB security guidance on Rules of Behavior)
DCAAR 4140.2 Use of Government Office Equipment, February 11, 2000
DCAAR 5025.11 DCAA Electronic Mail System, May 23, 2001
DODD 8500.1 Information Assurance, October 24, 2002
DODD O-8530.1 Computer Network Defense (CND), January 8, 2001
DODI 8500.2 Information Assurance Implementation, February 6, 2003
CJCSI 6510.01C Information Assurance and Computer Network Defense, May 1, 2001
CJCSM 6510.01 Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND), March 25, 2003
DODD 8100.02 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid, April 14, 2004
DOD Memorandum, Policy on Use of DoD Information Systems – Standard Consent Banner and User Agreement, May 9, 2008

Standard Mandatory Notice and Consent Provision for All DoD Information System User Agreements:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
- You consent to the following conditions:
    - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
    - At any time, the U.S. Government may inspect and seize data stored on this information system.

- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
    - The user consents to interception/capture and seizure of all communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
    - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
    - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
    - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

General Rules for Computer Users

Government equipment and software or contract related support equipment and software is provided to users to perform assigned work related tasks.

Authorized Users Shall:

- Take reasonable precautions to protect and avoid loss or damage to government or contract support equipment and software.
- Not leave a workstation or any other computer device (e.g., server, router) unattended without locking access.
- Hold U.S. Government security clearances or reviews commensurate with the level of information to which they are being granted access.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.
- Immediately report all Information Assurance (IA) - related events and potential threats and vulnerabilities involving an information system or enclave to the appropriate Information Assurance Officer (IAO) (formerly ISSO).
- Protect their authenticators (UserIDs, passwords, PKI certificates, Common Access Cards, etc.) and report any compromise or suspected compromise of an authenticator to the appropriate IAO. Passwords are not to be shared.
- Ensure that system media and output are properly classified, marked, controlled, stored, transported, and destroyed.

- Protect terminals or workstations from unauthorized access.
- Observe rules and regulations governing the secure operation and authorized use of an information system or enclave.
- Use the information system or enclave only for authorized purposes.
- Not introduce malicious code into any information system or enclave or physically damage the system or enclave (e.g., scan diskette and other media files for viruses).
- Not play unauthorized media (Example: CD's, DVD's, MP3 players) on government computer equipment (to avoid imbedded malicious code).
- Not bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed for any reason, users shall coordinate the procedure with the IAO and receive written permission from the Information Assurance Manager (IAM) (formerly the ISSM) for the procedure.
- Not introduce or use unauthorized software, firmware, or hardware onto the system or enclave.
- Not relocate or change information system or enclave equipment or the network connectivity of equipment without proper IA authorization.

Internet Rules for Computer Users

Guidance

- Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) that they are using. Acceptable practices are listed below.
- Users have a responsibility to employ available security mechanisms and procedures for protecting their data and assisting in the protection of systems they use.
- Users' outbound communications must not be inflammatory, harassing, defamatory, or disruptive to other's operations or otherwise reflect poorly on the DCAA's or Federal Government's reputation or image.
- Users are specifically advised that they should have no expectation of privacy for any Internet communications, whether business or personal. Further, user communications passing through government communications channels may be intercepted and/or monitored. Any violations of law identified by DCAA will be reported to law enforcement officials.
- Sensitive or Privacy Act information should not be sent onto the public Internet unless it is encrypted.

Acceptable Uses of the Internet

- Users may conduct DCAA business as required in accordance with official DCAA missions and functions and the users assigned work responsibilities.
- Users may perform work related research and analysis.
- Users may remain professionally current through the communication and exchange of information relating to the users professional field. Work related professional associations are included.

Unacceptable Uses of the Internet

- Users must not conduct for-profit activities not sanctioned by DCAA (e.g., operating or supporting a private business using government resources or time).
- Users must not establish personal email accounts on a DCAA computer (e.g., a hotmail account accessed from the office).
- Users must not establish a personal Internet account on a DCAA computer.
- Users must not access illegal or inappropriate sites such as hate speech or material that ridicules others based on race, creed, religion, color, sex, age, disability, national origin, or sexual orientation.
- Users must not access DCAA networks and computers from a non-government provided computer (e.g., from a personal computer at home, from a contractor provided computer).
- Users must not seek or gain unauthorized access to resources of the Internet (e.g., to attempt or succeed in obtaining unauthorized access into another network or computer).
- Users must not download or connect to sites providing non work related streaming audio or video (e.g., downloading MP3 music files into a DCAA computer).
- Users must not alter or destroy the integrity (e.g., unauthorized content change, addition or deletion) of computer based information.
- Users must not compromise the privacy of users or data.
- Users must not download or view pornography (i.e., sexually explicit or sexually oriented materials).
- Users must not play computer games.

_____

Authorized User

_____

Date Signed

_____

Supervisor

_____

Date Signed